Internet of Things

ENOG 14, Minsk, BY, 2017-10-10

http://slides.cabo.space
Carsten Bormann

Universität Bremen TZI
IETF CoRE WG
IRTF T2T RG

http://slides.cabo.space
<table>
<thead>
<tr>
<th>RFC 2429</th>
<th>RFC 2509</th>
<th>RFC 2686</th>
<th>RFC 2687</th>
<th>RFC 2689</th>
<th>RFC 3095</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3189</td>
<td>RFC 3190</td>
<td>RFC 3241</td>
<td>RFC 3320</td>
<td>RFC 3485</td>
<td>RFC 3544</td>
</tr>
<tr>
<td>RFC 3819</td>
<td>RFC 3940</td>
<td>RFC 3941</td>
<td>RFC 4629</td>
<td>RFC 5049</td>
<td>RFC 5401</td>
</tr>
<tr>
<td>RFC 5740</td>
<td>RFC 5856</td>
<td>RFC 5857</td>
<td>RFC 5858</td>
<td>RFC 6469</td>
<td>RFC 6606</td>
</tr>
<tr>
<td>RFC 6775</td>
<td>RFC 7049</td>
<td>RFC 7228</td>
<td>RFC 7252</td>
<td>RFC 7400</td>
<td>RFC 7959</td>
</tr>
<tr>
<td>RFC 8132</td>
<td>RFC 8138</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Bringing the Internet to new applications

- “Application X will never run on the Internet”
- ...
- ...
- “How do we turn off the remaining parts of X that still aren’t on the Internet”? 
Internet of Things

Scale up:

Number of nodes

(xx billion by 2020)
Internet of Things

Scale down:

node
Internet of Things

Scale down:

cost
complexity
cent kilobyte megahertz
There is not just a single class of “constrained node”

Class 0: too small to securely run on the Internet
   ✘ “too constrained”

Class 1: ~10 KiB data, ~100 KiB code
   ✔ “quite constrained”, “10/100”

Class 2: ~50 KiB data, ~250 KiB code
   ✔ “not so constrained”, “50/250”

These classes are not clear-cut, but may structure the discussion and help avoid talking at cross-purposes.
Internet of Things?

IP = Internet Protocol
“IP is important”
IP = Integration Protocol
IP: drastically reducing barriers

- **IP telephony** (1990s to 2018): replaced much of the special telephony hardware by routers and servers
  - several orders of magnitude in cost reduction
  - available programmer pool increases massively
  - What started as convergence, turned into *conversion*
- Everything is **not** the special snowflake it is said to be
- **Now:** *Internet of Things*
<table>
<thead>
<tr>
<th>Hype-IoT</th>
<th>Real IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4, NATs</td>
<td>IPv6</td>
</tr>
<tr>
<td>Device-to-Cloud</td>
<td>Internet</td>
</tr>
<tr>
<td>Gateways, Silos</td>
<td>Small Things Loosely Joined</td>
</tr>
<tr>
<td>Questionable Security</td>
<td>Real Security</td>
</tr>
<tr>
<td>$40+</td>
<td>&lt; $5</td>
</tr>
<tr>
<td>W</td>
<td>mW, µW</td>
</tr>
</tbody>
</table>
IoT: Current Deployment Models

- **Device to cloud**
  - Add isolated nodes to existing LANs (e.g., WiFi)
  - Lots of “ants” (v4: You might see this in your CGNs)
  - v4: Reachability from outside requires keepalive (often UDP!)
- **Device to “gateway”/hub** (...to cloud)
  - Closer to other traffic we have today
  - Adds more periodic microflows to the mix
- **Device to device** (“thing-to-thing”, general Internet connectivity)
  - (v4: Behind the NAT, or lots of hole punching needed)

[RFC 7452]
… a properly networked world … could be safer, greener, more efficient and more productive … But in order for that to emerge, the system has to be designed in the way that the internet was designed in the 1970s – by engineers who know what they’re doing, setting the protocols and technical standards that will bring some kind of order and security into the chaos of a technological stampede.

John Naughton, “The internet of things needs better-made things” (The Guardian, 2016-07-10)
We make the net work.
<table>
<thead>
<tr>
<th>INT</th>
<th>LWIG</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>INT</td>
<td>6LoWPAN</td>
<td>IP over 802.15.4</td>
</tr>
<tr>
<td>INT</td>
<td>6Lo</td>
<td>IP-over-foo</td>
</tr>
<tr>
<td>INT</td>
<td>6TiSCH</td>
<td>IP over TSCH</td>
</tr>
<tr>
<td>INT</td>
<td>LPWAN</td>
<td>Low-Power WAN Networks</td>
</tr>
<tr>
<td>RTG</td>
<td>ROLL</td>
<td>Routing (RPL)</td>
</tr>
<tr>
<td>APP</td>
<td>CoRE</td>
<td>REST (CoAP) + Ops</td>
</tr>
<tr>
<td>APP</td>
<td>CBOR</td>
<td>CBOR &amp; CDDL</td>
</tr>
<tr>
<td>SEC</td>
<td>DICE</td>
<td>Improving DTLS</td>
</tr>
<tr>
<td>SEC</td>
<td>ACE</td>
<td>Constrained AA</td>
</tr>
<tr>
<td>SEC</td>
<td>COSE</td>
<td>Object Security</td>
</tr>
<tr>
<td>Technology</td>
<td>Traits</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.15.4 (&quot;ZigBee&quot;)</td>
<td>Many SoCs, 0.9 or 2.4 GHz, 6TiSCH upcoming</td>
<td></td>
</tr>
<tr>
<td>BlueTooth Smart</td>
<td>On every Phone</td>
<td></td>
</tr>
<tr>
<td>DECT ULE</td>
<td>Dedicated Spectrum, In every home gateway</td>
<td></td>
</tr>
<tr>
<td>ITU-T G.9959 (&quot;Z-Wave&quot;)</td>
<td>Popular @home</td>
<td></td>
</tr>
<tr>
<td>802.11ah (&quot;HaLow&quot;)</td>
<td>Low power &quot;WiFi&quot;</td>
<td></td>
</tr>
<tr>
<td>NFC</td>
<td>Proximity</td>
<td></td>
</tr>
<tr>
<td>6lobac</td>
<td>Wired (RS485)</td>
<td></td>
</tr>
<tr>
<td>IEEE 1901.2 (LF PLC)</td>
<td>Reuses mains power lines</td>
<td></td>
</tr>
<tr>
<td>Ethernet + PoE</td>
<td>Wired, supplies 12–60 W</td>
<td></td>
</tr>
<tr>
<td>WiFi, LTE, …</td>
<td>Power?</td>
<td></td>
</tr>
</tbody>
</table>
Application Layer Protocols

- CoRE: Constrained RESTful Environments: Replace HTTP by a less expensive equivalent (CoAP)
  - From special-purpose/siloed to general purpose

- ACE: Define Security less dependent on humans in the loop and on very fast upgrade cycles
  - Embrace the multi-stakeholder IoT
Application Layer Data Formats

- Industry move to **JSON** for data interchange
- Add **CBOR** where JSON is too expensive
- Use **JOSE** and **COSE** as the security formats
- Work on semantic interoperability (IRTF **T2TRG**), with W3C, OCF, OMA/IPSO (LWM2M), iot.schema.org, … → self-description
Reducing TCO: Self-Description and Discovery

- Manually setting up $10^{11}$ nodes is a non-starter

- **Self-Description:**
  IoT nodes support automatic integration
  - RFC 6690 /.well-known/core “link-format”
  - W3C WoT work on “Thing Description” ongoing
  - **Semantic Interoperability!**

- **Discovery:**
  IoT nodes and their peers can find others
  - /.well-known/core exposes resources of a node
  - **Resource Directories** (with a bridge to DNS-SD)
IoT Devices as a secure application
Protect the objectives right ✔

vs.

Protect the right objectives 🌶
Now let’s apply all this to constrained devices
Constrained Level
authentication and authorization requests resource
provides resource

S
C

authenticated
authorization support

SOP

in charge of

Overs. Principal Level: Individuals / Companies

Server Owner's Security Domain

Less-Constrained Level

authenticating
authorization support

COP

Client Owner's Security Domain

requests resource
provides resource

CAM

security domain

SAM

Constrained Level

C
S
Shaping the Security Workflows

- Stakeholders, Principals
- Less-constrained nodes
- Constrained nodes
- Device Lifecycle
- Authorized, authenticated delegation
IoT Devices as an attack platform
user duty

garage?
vendor duty

CE • regulation? • UL
• Protect the network and other unrelated users against an IoT Device that may be insecure
• Idea: Document expected behavior in an actionable way
• MUD as standardized today:
  Can be used for firewall configuration
    ‣ Poke firewall holes for desirable traffic
    ‣ Detect when the IoT Device has been compromised
• Where can we take this idea?
Software Updates are needed

• Bugs are being found
• Environments change

⇒ Update or discard!

• Traditional: manual upgrade by connecting a special upgrader device (e.g., PC with upgrader app)
  • Too expensive; device might be hard to reach
• Needed: Secure Over-the-air Upgrade
If it is not *usably secure*, it’s not the *Internet of Things*